additional information, such as attributes of the system used by the first user, such as a serial number uniquely identifying the processor or operating system (or both). Unfortunately, however, the first user can no longer access the content on another system.

A need therefore exists for a method and apparatus for limiting access to content to an authorized user on a number of systems. A further need exists for a digital watermarking technique that allows an authorized user to be uniquely identified.

Generally, a method and apparatus are that restrict access to digital content to an authorized user on one or more systems using biometric watermarks. The disclosed biometric watermarking techniques allow an authorized user to be uniquely identified. Access to digital content is restricted to digital content in accordance with the present invention by embedding a biometric watermark, such as a biometric image, in the content. Thereafter, a user can only access the content if a biometric sample of the user matches the embedded biometric watermark. In one variation, the user can only access the content if the biometric sample is a live biometric sample.

The embedded biometric watermark optionally includes information describing a system employed by the user to obtain the content. The user can optionally be permitted to access the content, without a biometric evaluation, if the content is on a system that has been previously authorized for the user using a biometric evaluation.

A more complete understanding of the present invention, as well as further features and advantages of the present invention, will be obtained by reference to the following detailed description and drawings.

FIG. 1 illustrates a conventional system for embedding and detecting watermarks in digital content;

FIG. 2 illustrates a conventional content access device incorporating features of the present invention;

FIG. 3 is a flow chart of an exemplary watermark encoding process incorporating features of the present invention; and

FIG. 4 is a flow chart of an exemplary watermark detection process incorporating features of the present invention.

FIG. 1 illustrates a conventional watermark encoding and detection system 100. Content data 110 is processed by watermark encoding processor 120 to add a watermark 115 to the content data 110. Algorithms for embedding watermarks are well known in the art. For a detailed discussion of a suitable watermark encoding algorithm, see, for example, International Patent No. WO 08/091375, entitled "Watermarking," incorporated by reference herein. The watermarked content 130 is then distributed via one or more of methods, including networks, DVDs, or CDs (or a combination of the foregoing). A content access device 200, discussed further below in conjunction with FIG. 2, such as a DVD player, is then utilized to play-out the watermarked content 130.

FIG. 2 illustrates a conventional content access device 200. The content access device 200 may be embodied, for example, as any conventional content access device, such as a commercially available DVD player, as modified herein to provide the features and functions of the present invention. As shown in FIG. 2, content data input device 215 accesses content data 130 for presentation, for example, from memory, a DVD or CD. The output device 230 may be, for example, a display or speaker (or a combination thereof) for presenting visual or audio information, respectively. Content data processor 220 transforms the content data 130 for display by output device 230. As the content data 130 is accessed, watermark detector 210 repeatedly searches for a valid watermark 115. A valid watermark 115 is a watermark that has not been altered beyond a specified threshold from its original form. If a valid watermark 115 with its proper payload is detected, watermark detector 210 signals content data processor 220 to continue to process and output content data 240. If watermark detector 210 detects a corrupted watermark 115 (or an improper watermark payload), watermark detector 210 signals content data processor 220 to halt the play-out of output content data 240. A corrupted watermark 115 is a watermark that has been transformed from its original form by one or more techniques, such as rotating the original watermark 90 degrees from its initial orientation. For a more detailed discussion of suitable techniques for detecting watermarks in content, see, for example, International Patent No. WO 01/91461, entitled "Watermark Detection," incorporated by reference herein.

According to one aspect of the present invention, access to multimedia content is restricted using biometric watermarks. For example, when a first user legally obtains a copy of the content from a service provider, a biometric associated with the first user is embedded into the content. The biometric watermark may include, for example, a finger print, speech pattern, iris pattern, or facial image. Since biometrics taken from the same user at different times vary and their recognition is not guaranteed, multiple instances of the biometric can be taken and embedded into the content.

In one exemplary implementation, when a user obtains content, a biometric identifier is obtained from the user, as well as one or more parameters identifying a system of the user. Each time the biometric is embedded into the content, the system information can also be embedded. Thereafter, whenever the user attempts to access the content, the user is requested to provide a biometric identifier. The provided biometric information is compared to the biometric information embedded in the content. If the provided biometric information matches the embedded biometric information, the user will be allowed to access the content. In this manner, the authorized user cannot share the content with another user, since the second user generally would not have the biometric or system information of the authorized user.

According to a further aspect of the present invention, the user can transfer the downloaded content to a different system, by satisfying a biometric evaluation on the new machine. In one variation of the invention, once the content is authorized for the user on a given system, further biometric comparisons can optionally be suspended whenever the same content is played on the same system. The present invention provides a mechanism for identifying the user that has been the source of pirated content.

In yet another variation, the authorized user can be required to provide a "live" biometric. In other words, the present invention can ensure that the authorized user is providing a live biometric and not a biometric that has been previously stored. For a discussion of suitable techniques for detecting if a biometric is live, see, for example, R. Derakhshani et al. "Determination of Vitality from a Non-Invasive Biomedical Measurement for use in Fingerprint Scanners," Pattern Recognition, vol. 17, no. 2, (2003), or S.A.C. Schuckers, "Spoofing and Anti-Spoofing Measures,"